IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
Before the Board of Patent Appeals and Interferences

In re Patent Application of

SIMPSON et al

Serial No. 10/088,541

Filed: March 19, 2002

Title: METHOD FOR COMPUTER SECURITY

Atty Dkt. SCS-124-928
C# M#

TC/A.U.: 2132

Examiner: B. Bludau

Date: August 20, 2007

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

☐ **Correspondence Address Indication Form Attached.**

☐ **NOTICE OF APPEAL**
Applicant hereby **appeals** to the Board of Patent Appeals and Interferences from the last decision of the Examiner twice/finally rejecting applicant's claim(s). $500.00 (1401)/$250.00 (2401) $

☒ An appeal **BRIEF** is attached in the pending appeal of the above-identified application $500.00 (1402)/$250.00 (2402) $ 500.00

☐ Credit for fees paid in prior appeal without decision on merits -$ ( )

☐ A reply brief is attached. **(no fee)**

☐ Petition is hereby made to extend the current due date so as to cover the filing date of this paper and attachment(s)
One Month Extension $120.00 (1251)/$60.00 (2251)
Two Month Extensions $450.00 (1252)/$225.00 (2252)
Three Month Extensions $1020.00 (1253/$510.00 (2253)
Four Month Extensions $1590.00 (1254/$795.00 (2254) $

☐ "Small entity" statement attached.

Less month extension previously paid on -$( )

TOTAL FEE ENCLOSED $ 500.00

Any future submission requiring an extension of time is hereby stated to include a petition for such time extension. The Commissioner is hereby authorized to charge any deficiency, or credit any overpayment, in the fee(s) filed, or asserted to be filed, or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our **Account No. 14-1140.** A duplicate copy of this sheet is attached.

901 North Glebe Road, 11th Floor
Arlington, Virginia 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100
SCS:kmm

NIXON & VANDERHYE P.C.
By Atty: Stanley C. Spooner, Reg. No. 27,393

Signature: _____

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Patent Application of
SIMPSON et al
Serial No. 10/088,541
Filed: March 19, 2002
For: METHOD FOR COMPUTER SECURITY

Confirmation No.: 6928
Atty. Ref.: 124-928
Group: 2132
Examiner: B. Lanier

* *

APPEAL BRIEF

On Appeal From Group Art Unit 2132

Stanley C. Spooner
NIXON & VANDERHYE P.C.
11th Floor, 901 North Glebe Road
Arlington, Virginia 22203
(703) 816-4028
Attorney for Appellant

TABLE OF CONTENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Patent Application of

SIMPSON et al — Atty. Ref.: 124-928

Serial No. 10/088,541 — Group: 2132

Filed: March 19, 2002 — Examiner: B. Bludau

For: METHOD FOR COMPUTER SECURITY

* *

August 20, 2007

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

I. REAL PARTY IN INTEREST

The real party in interest in the above-identified appeal is QinetiQ Limited by virtue of an assignment of rights from the inventors to QinetiQ Limited recorded March 19, 2002 at Reel 12905, Frame 296.

II. RELATED APPEALS AND INTERFERENCES

There are believed to be no related appeals, interferences or judicial proceedings with respect to the present application, other than the Pre-Appeal Brief Request for Review previously filed in this appeal on April 26, 2007.

III. STATUS OF CLAIMS

Claims 1-45 stand rejected in the Final Official Action. The Examiner contends that with respect to claims 1-45, they are obvious in view of Baker (U.S. Patent 5,695,898) in view of David ("An Implementation of MLS on a Network of Workstations Using X.500/509") as combined themselves or in various combinations with Hsiao (U.S. Patent 6,496,944), Harn ("ID-Based Cryptographic Schemes for User Identification, Digital Signature, and Key Distribution"), McNabb (U.S. Patent 6,289,462), Hayman (U.S. Patent 5,859,966) and Netscape ("Netscape Messaging Server Version 3.0 Administrator's Guide"). The above rejections of claims 1-45 are appealed.

IV. STATUS OF AMENDMENTS

No further response has been submitted with respect to the Final Official Action in this application other than the filing of a Pre-Appeal Brief Request for Review which decision was mailed July 13, 2007.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

Appellants' specification and figures provide an explanation of the claimed invention set out in independent claims 1, 19, 32, 35, 38, 40, 41, 43, 44 and 45, with each claimed structure, program logic and method step addressed as to its location in the specification and in the figures.

"1. (currently amended) A method for computer security to control access to data held on a computer system [web server 2 as shown in Figure 1 and discussed on page 9, line 20 through page 14, line 14 and elsewhere in the specification] as requestable datasets [web pages 4 as shown in Figure 1 and discussed on page 9, line 20 through page 12, line 15 and elsewhere in the specification], said method comprising the steps of:

allocating human users of a computer system [external client computer 12 as shown in Figure 1 and discussed on page 10, lines 1-11 and elsewhere in the specification] between a plurality of user groups [e.g. Personnel, Research as shown in Figure 2 and discussed on page 14, lines 15-30 and elsewhere in the specification] as members thereof wherein not all user groups have only a single member and membership of a user group having multiple members is authentically evidenced by provision of user group identity information [X.509 certificate 20 as shown in Figure 2 and discussed on page 14, line 15 through page 16, line 18 and elsewhere in the specification] common to such members, each user group corresponding to a respective dataset access category [Access Control List 10 and Security Label, e.g., 45433 as shown in Figure 2 and discussed on page 11, line 29 through page 12, line 10, page 12, line 22 through page 13, line 7 and elsewhere in the specification] selected from a plurality of such categories such that all members of each user group having multiple members are

associated with a dataset access category which is common to members of that user group;

providing for each dataset [web pages 4] a dataset access category [Access Control List 10 and Security Label] selected from said plurality of such categories and associated with a criterion [Security Rating UNCLASS in Access Control List 10 as shown in Figure 2 and discussed on page 12, line 22 through page 14, line 30 and elsewhere in the specification] for access to that dataset by computer system users; and

giving access to a dataset [web pages 4] to a member of a user group [e.g., Personnel, Research] with multiple members in response to such member providing authenticated evidence [X.509 Certificate 20] of membership of that user group and members of that user group being associated with a common dataset access category [Access Control List 10 and Security Label] which enables access to that dataset [web pages 4]."

"19. (currently amended) A computer program product comprising a computer readable medium containing computer readable instructions for controlling operation of a computer system [external client computer 12 as shown in Figure 1 and discussed on page 10, lines 1-11 and elsewhere in the specification] and providing control of access to data held on a computer system [web server 2 as shown in Figure 1 and discussed on page 9, line 20 through page

14, line 14 and elsewhere in the specification] as requestable datasets [web pages 4 as shown in Figure 1 and discussed on page 9, line 20 through page 12, line 15 and elsewhere in the specification] each having an access category selected from a plurality of such categories [Access Control List 10 and Security Label, e.g., 45433 as shown in Figure 2 and discussed on page 11, line 29 through page 12, line 10, page 12, line 22 through page 13, line 7 and elsewhere in the specification] and associated with a criterion [Security Rating UNCLASS in Access Control List 10 as shown in Figure 2 and discussed on page 12, line 22 through page 14, line 30 and elsewhere in the specification] for access to that dataset by computer system users, wherein the computer readable instructions provide a means for controlling the computer system to:

(a) receive data requests [16r, 18r, 8r as shown in Figure 3 and discussed on page 15, lines 1-6 and elsewhere in the specification] from human users of a computer system [external client computer 12] allocated between a plurality of user groups [e.g. Personnel, Research as shown in Figure 2 and discussed on page 14, lines 15-30 and elsewhere in the specification] as members thereof wherein not all user groups have only a single member and membership of a user group having multiple members is authentically evidenced by provision of user group identity information [X.509 certificate 20 as shown in Figure 2 and discussed on page 14, line 15 through page 16, line 18 and elsewhere in the specification] common to such members, each user group being associated

with a respective one of said data access categories [Access Control List 10 and Security Label] such that all members of a user group having multiple members are associated with a dataset access category which is common to members of that user group;

(b) control access to datasets [web pages 4] each of which is associated with a dataset access category [Access Control List 10 and Security Label] selected from said plurality of such categories and associated with a criterion [Security Rating UNCLASS] for access to that dataset by computer system users; and

(c) give access to a dataset [web pages 4] to a member of a user group [e.g. Personnel, Research] with multiple members in response to such member providing authenticated evidence[X.509 certificate 20] of membership of that user group and members of that user group being associated with a common dataset access category [Access Control List 10 and Security Label] which enables access to that dataset [web page 4]."

"32. (currently amended) A network access controller for controlling access to data held on a computer system [web server 2 as shown in Figure 1 and discussed on page 9, line 20 through page 14, line 14 and elsewhere in the specification] as requestable datasets [web pages 4 as shown in Figure 1 and

discussed on page 9, line 20 through page 12, line 15 and elsewhere in the specification], wherein the controller:

(a) receives data requests [16r, 18r, 8r as shown in Figure 3 and discussed on page 15, lines 1-6 and elsewhere in the specification] from human users of a computer system [external client computer 12 as shown in Figure 1 and discussed on page 10, lines 1-11 and elsewhere in the specification] allocated between a plurality of user groups [e.g. Personnel, Research as shown in Figure 2 and discussed on page 14, lines 15-30 and elsewhere in the specification] as members thereof wherein not all user groups have only a single member and membership of a user group having multiple members is authentically evidenced by provision of user group identity information [X.509 certificate 20 as shown in Figure 2 and discussed on page 14, line 15 through page 16, line 18 and elsewhere in the specification] common to such members, each user group corresponding to a respective dataset access category [Access Control List 10 and Security Label, e.g., 45433 as shown in Figure 2 and discussed on page 11, line 29 through page 12, line 10, page 12, line 22 through page 13, line 7 and elsewhere in the specification] selected from a plurality of such categories such that all members of each user group having multiple members are associated with a dataset access category [Access Control List 10 and Security Label] which is common to members of that user group;

(b) controls access to datasets [web pages 4] each of which is associated with a dataset access category [Access Control List 10 and Security Label] selected from said plurality of such categories and associated with a criterion [Security Rating UNCLASS in Access Control List 10 as shown in Figure 2 and discussed on page 12, line 22 through page 14, line 30 and elsewhere in the specification] for access to that dataset by computer system users; and

(c) gives access to a dataset [web pages 4] to a member of a user group [e.g., Personnel, Research] with multiple members in response to such member providing authenticated evidence [X.509 Certificate 20] of membership of that user group and members of that user group being associated with a common dataset access category [Access Control List 10 and Security Label] which enables access to that dataset [web pages 4]."

"35. (currently amended) A computer network for database access by human users having identifying certificates [X.509 certificate 20 as shown in Figure 2 and discussed on page 14, line 15 through page 16, line 18 and elsewhere in the specification] and allocated between a plurality of user groups [e.g. Personnel, Research as shown in Figure 2 and discussed on page 14, lines 15-30 and elsewhere in the specification] as members thereof wherein not all user groups have only a single member and membership of a user group having multiple members is authentically evidenced by provision of user group identifying

certificate information [X.509 certificate 20] common to such members, wherein said network treats each user group as corresponding to a respective dataset access category [Access Control List 10 and Security Label, e.g., 45433 as shown in Figure 2 and discussed on page 11, line 29 through page 12, line 10, page 12, line 22 through page 13, line 7 and elsewhere in the specification] selected from a plurality of such categories such that all members of each user group having multiple members are associated with a dataset access category which is common to members of that user group, and includes:

(a) an access controller [computer system 6 shown in Figure 1 and discussed on page 9, lines 20-30 and elsewhere in the specification] controlling access to a database comprising a plurality of datasets [web pages 4 as shown in Figure 1 and discussed on page 9, line 20 through page 12, line 15 and elsewhere in the specification] each having an associated dataset access category [Access Control List 10 and Security Label, e.g., 45433 as shown in Figure 2 and discussed on page 11, line 29 through page 12, line 10, page 12, line 22 through page 13, line 7 and elsewhere in the specification] selected from said plurality of such categories and associated with a criterion [Security Rating UNCLASS in Access Control List 10 as shown in Figure 2 and discussed on page 12, line 22 through page 14, line 30 and elsewhere in the specification] for access to that dataset by users;

(b) means for verifying human users [Access Control List 10 as shown in Figure 1 and discussed on page 9, lines 20-30, page 11, lines 16-27, page 12, line 22 through page 13, line 7 and elsewhere in the specification];

(c) a database of datasets [web pages 4] each of which is associated with a dataset access category selected from said plurality of such categories [Access Control List 10 and Security Label]; and

(d) computer software arranged to give access to a dataset [web page 4] to a member of a user group with multiple members in response to such member providing identifying certificate information [X.509 certificate 20] as evidence of membership of that user group and members of that user group being associated with a common dataset access category [Access Control List 10 and Security Label] which enables access to that dataset."

"38. (currently amended) A method for controlling user access to data held on a computer system [web server 2 as shown in Figure 1 and discussed on page 9, line 20 through page 14, line 14 and elsewhere in the specification] as requestable datasets [web pages 4 as shown in Figure 1 and discussed on page 9, line 20 through page 12, line 15 and elsewhere in the specification], the method including:

labelling the datasets [dataset 110 shown in Figure 6 and discussed on page 22, line 13 to page 23, line 2 and elsewhere in the specification] with dataset access labels [dataset labels 112 shown in Figure 6 and discussed on

page 22, line 13 to page 23, line 2 and elsewhere in the specification] defining a hierarchy of data access levels each associated with a criterion [Security Rating UNCLASS in Access Control List 10 as shown in Figure 2 and discussed on page 12, line 22 through page 14, line 30 and elsewhere in the specification] for access to a dataset [dataset 110] by computer system users,

allocating human users of a computer system [external client computer 12 as shown in Figure 1 and discussed on page 10, lines 1-11 and elsewhere in the specification] between a plurality of user groups [e.g. Personnel, Research as shown in Figure 2 and discussed on page 14, lines 15-30 and elsewhere in the specification] as members thereof wherein not all user groups have only a single member and membership of a user group having multiple members is authentically evidenced by provision of user group identity information [X.509 certificate 20 as shown in Figure 2 and discussed on page 14, line 15 through page 16, line 18 and elsewhere in the specification] common to such members,

labelling user groups [e.g. Personnel, Research] with data access levels selected from said plurality thereof such that all members of each user group having multiple members are associated with a dataset access level which is common to members of that user group; and

giving access to a requested dataset [web pages 4] to a requesting member of a user group with multiple members in response to such member providing authenticated evidence [X.509 Certificate] of membership of that user group and

members of that user group being labelled with a common data access level which in the hierarchy is equal to or above the dataset access level of the requested dataset."

"40. (currently amended) A method for controlling user access to data held on a computer system [web server 2 as shown in Figure 1 and discussed on page 9, line 20 through page 14, line 14 and elsewhere in the specification] as requestable web pages [web pages 4 as shown in Figure 1 and discussed on page 9, line 20 through page 12, line 15 and elsewhere in the specification], the method including:

(a) labelling the web pages with meta tags defining a hierarchy of data access levels [dataset labels 112 shown in Figure 6 and discussed on page 22, line 13 to page 23, line 2 and elsewhere in the specification] for an access control list providing a plurality of data access levels each associated with a criterion [Security Rating UNCLASS in Access Control List 10 as shown in Figure 2 and discussed on page 12, line 22 through page 14, line 30 and elsewhere in the specification] for access to a dataset by computer system users,

(b) allocating human users of a computer system [external client computer 12 as shown in Figure 1 and discussed on page 10, lines 1-11 and elsewhere in the specification] between a plurality of user groups [e.g. Personnel, Research as shown in Figure 2 and discussed on page 14, lines 15-30 and elsewhere in the

specification] as members thereof wherein not all user groups have only a single member and membership of a user group having multiple members is authentically evidenced by provision of user group identity information [X.509 certificate 20 as shown in Figure 2 and discussed on page 14, line 15 through page 16, line 18 and elsewhere in the specification] common to such members, each member having a key for signing data and a certificate indicating groupings to which that member belongs,

(c) labelling user groups [e.g. Personnel, Research] with respective data access levels associated with member groupings and selected from said plurality thereof such that all members of each user group having multiple members are associated with a dataset access level which is common to members of that user group,

(d) using a proxy server to:

receive a request for a web page from a client computer system [external client computer 12] having web browser software [web browser 16 shown in Figure 1 and discussed on page 10, lines 1-11 and elsewhere in the specification] and client proxy software and controlled by a requesting member of a user group,

send data for signature to the client computer system and obtain the requesting member's certificate,

receive data from the client computer system,

verify that the received data is:

(1) signed with the requesting member's key,

(2) a signed equivalent of the data sent to the requesting member for signature, and

(3) signed with a key from a certificate which is not time expired or invalid,

if the received data is verified as aforesaid, check the data access level of the requesting member's user group against the access control list, and

give access to a requested web page to the requesting member if said requesting member is a member of a user group with multiple members in response to such member providing authenticated evidence of membership of that user group and members of that user group being labelled with a common data access level which in the hierarchy is equal to or above the dataset access level of the requested web page."

"41. (previously presented) A network access control system for controlling access to data held on a computer system as requestable datasets [web pages 4 as shown in Figure 1 and discussed on page 9, line 20 through page 12, line 15 and elsewhere in the specification], the control system being arranged to:

(a) label the datasets [dataset 110 shown in Figure 6 and discussed on page 22, line 13 to page 23, line 2 and elsewhere in the specification] with dataset access labels [dataset labels 112 shown in Figure 6 and discussed on page 22, line 13 to page 23, line 2 and elsewhere in the specification] defining a hierarchy of data access levels,

(b) communicate with human computer system users allocated between a plurality of human user groups [e.g., Personnel, Research as shown in Figure 2 and discussed on page 14, lines 15-30 and elsewhere in the specification],

(c) label said user groups [e.g., Personnel, Research] with data access levels selected from a plurality of such levels; and

(d) give access to a requested dataset [e.g. Personnel, Research as shown in Figure 2 and discussed on page 14, lines 15-30 and elsewhere in the specification] to a requesting human member of a user group labelled with a data access level which in the hierarchy is equal to or above the data access level of the requested dataset."

"43. (currently amended) A network access control system for controlling user access to data held on a computer system as requestable web pages [web pages 4 as shown in Figure 1 and discussed on page 9, line 20 through page 12, line 15 and elsewhere in the specification], the control system being arranged to:

(a) label the web pages [dataset 110 shown in Figure 6 and discussed on page 22, line 13 to page 23, line 2 and elsewhere in the specification] with meta tags defining a hierarchy of data access levels [dataset labels 112 shown in Figure 6 and discussed on page 22, line 13 to page 23, line 2 and elsewhere in the specification] for an access control list providing a plurality of data access levels each associated with a criterion [Security Rating UNCLASS in Access Control List 10 as shown in Figure 2 and discussed on page 12, line 22 through page 14, line 30 and elsewhere in the specification] for access to a dataset by computer system users,

(b) allocate human users of a computer system between a plurality of user groups [e.g., Personnel, Research as shown in Figure 2 and discussed on page 14, lines 15-30 and elsewhere in the specification] as members thereof wherein not all user groups have only a single member and membership of a user group having multiple members is authentically evidenced by provision of user group identity information [X.509 certificate 20 as shown in Figure 2 and discussed on page 14, line 15 through page 16, line 18 and elsewhere in the specification] common to such members, each member having a key for signing data and a certificate indicating groupings to which that member belongs,

(c) label user groups [e.g., Personnel, Research] with respective data access levels associated with member groupings and selected from said plurality of member groupings such that all members of each user group having multiple

members are associated with a dataset access level which is common to members of that user group,

and the control system has a proxy server for:

(i) receiving a request for a web page from a client computer system having web browser software and client proxy software and controlled by a requesting member of a user group,

(ii) sending data for signature to the client computer system and obtain the requesting member's certificate,

(iii) receiving data from the client computer system,

(iv) verifying that the received data is:

signed with the requesting member's key,

a signed equivalent of the data sent to the requesting member for signature, and

signed with a key from a certificate which is not time expired or invalid,

(v) if the received data is verified as aforesaid, checking the data access level of the requesting member's user group against the access control list, and

(vi) giving access to a requested web page to the requesting member if it is a member of a user group with multiple members in response to such member providing authenticated evidence [X.509 Certificate] of membership of that user group and members of that user group being labelled with a common data access

level which in the hierarchy is equal to or above the dataset access level of the requested web page."

"44. (currently amended) A method for computer security to control access to data held on a computer system as requestable datasets, the method including:

(a) allocating human users of a computer system between a plurality of user groups [e.g., Personnel, Research as shown in Figure 2 and discussed on page 14, lines 15-30 and elsewhere in the specification] as members thereof wherein not all user groups have only a single member and membership of a user group having multiple members is authentically evidenced by provision of user group identity information [X.509 certificate 20 as shown in Figure 2 and discussed on page 14, line 15 through page 16, line 18 and elsewhere in the specification] common to such members;

(b) providing for each dataset [web pages 4 as shown in Figure 1 and discussed on page 9, line 20 through page 12, line 15 and elsewhere in the specification] an access category [Access Control List 10 and Security Label, e.g., 45433 as shown in Figure 2 and discussed on page 11, line 29 through page 12, line 10, page 12, line 22 through page 13, line 7 and elsewhere in the specification] selected from a plurality of such categories and associated with a criterion [Security Rating UNCLASS in Access Control List 10 as shown in Figure 2 and discussed on page 12, line 22 through page 14, line 30 and elsewhere

in the specification] for access to that dataset by computer system users, the dataset access categories being arranged in a hierarchy such that a relatively higher dataset access category incorporates one or more relatively lower dataset access categories;

(c) associating each user group with a respective dataset access category [Access Control List 10 and Security Label] such that all members of each user group having multiple members are associated with a dataset access category which is common to members of that user group and membership of a user group having multiple members is authentically evidenced by provision of like user group information [X.509 Certificate 20 as shown in Figure 2 and discussed on page 14, line 15 through page 16, line 18 and elsewhere in the specification] by each of such multiple members; and

(d) providing access to a dataset to a member of a user group with multiple members in response to such member providing authenticated evidence [X.509 Certificate] of membership of that user group and members of that user group being associated with a common dataset access category [Access Control List 10 and Security Label] which is in the hierarchy equal to or relatively higher than that required for access to that dataset."

"45. (currently amended) A method for computer security to control access to data held on a computer system [web server 2 as shown in Figure 1 and

discussed on page 9, line 20 through page 14, line 14 and elsewhere in the specification] as requestable datasets [web pages 4 as shown in Figure 1 and discussed on page 9, line 20 through page 12, line 15 and elsewhere in the specification], characterised in that the method includes:

(a) allocating human users of a computer system [external client computer 12 as shown in Figure 1 and discussed on page 10, lines 1-11 and elsewhere in the specification] between a plurality of user groups [e.g., Personnel, Research as shown in Figure 2 and discussed on page 14, lines 15-30 and elsewhere in the specification] as members thereof wherein not all user groups have only a single member and membership of a user group having multiple members is authentically evidenced by provision of user group identity information [X.509 Certificate 20 as shown in Figure 2 and discussed on page 14, line 15 through page 16, line 18 and elsewhere in the specification] common to such members;

(b) providing for each dataset [web page 4] an access category [Access Control List 10 and Security Label, e.g., 45433 as shown in Figure 2 and discussed on page 11, line 29 through page 12, line 10, page 12, line 22 through page 13, line 7 and elsewhere in the specification] selected from a plurality of such categories and associated with a criterion [Security Rating UNCLASS in Access Control List 10 as shown in Figure 2 and discussed on page 12, line 22 through page 14, line 30 and elsewhere in the specification] for access to that dataset by computer system users, the dataset access categories being arranged in a hierarchy

such that a relatively higher dataset access category incorporates one or more relatively lower dataset access categories;

(c) associating each user group with a respective dataset access category [Access Control List 10 and Security Label] such that all members of each user group having multiple members are associated with a dataset access category which is common to members of that user group;

(d) providing a respective computer-based identifying certificate means [X.509 Certificate 20] for each user containing said user group identity information; and

(e) providing access to a dataset to a member of a user group with multiple members in response to such member providing identifying certificate means [X.509 Certificate 20] and members of that user group being associated with a common dataset access category [Access Control List 10 and Security Label] which is in the hierarchy equal to or relatively higher than that required for access to that dataset."

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-5, 11-13, 17, 19-23, 29, 31, 32, 38, 41, 44 and 45 stand rejected under 35 USC §103 as unpatentable over Baker in view of Davis.

Claims 6, 24, 39 and 42 stand rejected under 35 USC §103 as being unpatentable over Baker and Davis in further view of Hsiao.

Claims 7 and 25 stand rejected under 35 USC §103 as unpatentable over Baker and Davis.

Claims 8, 9, 26 and 27 stand rejected under 35 USC §103 as unpatentable over Baker and Davis in further view of Harn.

Claims 10, 28 and 34 stand rejected under 35 USC §103 as unpatentable over Baker and Davis in further view of McNabb.

Claims 14-16, 30 and 33 stand rejected under 35 USC §103 as unpatentable over Baker and Davis in further view of Hayman.

Claim 18 stands rejected under 35 USC §103 as unpatentable over "Baker/Hayman" (Appellants believe Examiner meant to reference Baker/Davis/Hayman as previously applied to claim 16 in further view of Netscape).

Claim 35 stands rejected under 35 USC §103 as unpatentable over Baker and Davis.

VII. ARGUMENT

Each of Appellants' independent claims 1, 19, 32, 35, 38, 40, 41, 43, 44 and 45 recite method step, program logic or apparatus which are common among the independent claims. Various ones of these common elements are missing from the

Baker and Davis references and therefore the combination of Baker and Davis cannot render obvious any of these independent claims or claims dependent thereon.

The Examiner is reminded that the Court of Appeals for the Federal Circuit has held that "the PTO has the burden under Section 103 to establish a *prima facie* case of obviousness." *In re Fine*, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). "It can satisfy this burden only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the references."

With respect to the alleged motivation for combining these references, the Examiner has provided no support. In the recent case of *In re Rouffet* , 47 USPQ2d 1453, 1458 (Fed. Cir. 1998), the Court held that "the examiner must show reasons that the skilled artisan, confronted with the same problems as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner claimed." Nowhere in either of the cited references does there appear to be any recognition of the problem solved by the claimed invention.

A. The Examiner fails to identify any evidence of record tending to support an obviousness rejection of claims 1-5, 11-13, 17, 19-23, 29, 31, 32, 38, 41, 44 and 45 under §103 with respect to the Baker and Davis references

Claims 1-5, 11-13, 17, 19-23, 29, 31, 32, 38, 41, 44 and 45 stand rejected under 35 USC §103 as unpatentable over Baker in view of Davis. Appellants'

view is that neither Baker nor Davis teach a number of recited elements, logic steps and/or method steps which are recited in each of the independent claims.

As noted above, the Examiner, in order to satisfy his burden in establishing a *prima facie* case of obviousness, must show some "objective teaching in the prior art" of the claimed features and claimed interrelationships. As will be seen, the Examiner has failed to demonstrate where or how the prior art references teach the claimed features.

1. Baker fails to teach the claimed "allocating human users" step, logic or apparatus

All of Appellants independent claims require the step or the interrelationship of "allocating" human users between a plurality of user groups. This is not disclosed in the Baker reference.

The Examiner alleges that Baker at column 4, lines 36-46, 53-56, and column 5, lines 10-12 and 37-43 includes a disclosure of the claimed "allocating" step. The Examiner is in error. Col. 4, lines 36-46 discusses identification codes that are "user specific, as opposed to user terminal specific" passwords have nothing to do with the claimed allocating step. Col. 4, lines 53-56 discusses the operation when a user terminal transmits a request for access – again nothing to do with "allocating." Column 5, lines 10-12 discusses a listing of directories in which a user might be granted or denied access – nothing to do with an "allocating" step. Column 5, lines 37-43 discloses how the database allows students to view the "history resources"

database but not the "history answers" database – again, nothing to do with "allocating."

In fact, a review of column 1, lines 38-47 will establish that the only human groups Baker considers are **preexisting human groups** , i.e., groups of children, groups of parents and groups of employees. As a result, there is no allocating step in the Baker method. Since the burden is on the Examiner to show where this "allocating" step exists in Baker and, as yet , the Examiner has failed to meet his burden, there is no prima facie case of obviousness over Baker.

2. The independent claims specify the allocating step is with respect to "human users" and Baker fails to disclose this claimed feature

Appellants independent claims also specify in the allocating step, the allocation of "human users of a computer system." The Examiner suggests that Baker at column 4, line 65 to column 5, line 1 teaching "ID 207/208 is a single id that is common to users belong to that user group" and shows allocation among human users (Final Rejection, page 3). His contention is believed to be incorrect.

The reference to "ID 207/208" in Baker identifies two computer terminals in Figure 2. The sentence bridging columns 4 and 5 clarifies that the identification code $ID_{207/208}$ relates to terminals 207 and 208 and requires "when a URL from either user terminal 207 or 208 is received at processor 212, the same listing of associated URLs is accessed" (Baker, column 5, lines 1-3), i.e., both terminals are either granted or denied access to the same group of URLs.

However, as far as meeting the claim requirement of allocating "human users" there is no teaching as noted above. Baker merely teaches providing the same level of access to the two identified terminals. The burden is on the Examiner to show where this allocating "human users" step exists in Baker and, as yet , has failed to do so.

3. Baker fails to disclose any identification of "a data access category which is common to members of that user group"

Appellants' independent claims also require in the allocating step "all members of each user group having multiple members are associated with a dataset access category which is common to members of that user group." The Examiner alleges that this claim limitation is disclosed in Baker in columns 4 and 5 noted above. However, the above noted review of these cited portions of Baker confirms that Baker only discusses control of access to data **either** by restricting data which a terminal can access or by the use of a personal password unique to an individual and not by a dataset access category being common to human members of a user group.

The burden is on the Examiner to show where this allocating human user step "such that all members of each user group . . . are associated with a dataset access category which is common to members of that user group" exists in Baker. Because he has provided no evidence of such step, he has failed to establish a *prima facie* case of obviousness.

4. Neither Baker nor Davis teach providing access "in response to such member providing authenticated evidence of membership of that user group"

Appellants' independent claims require the "giving access" step to be "in response to such member providing authenticated evidence of membership of that user group." The Examiner alleges that this is disclosed in Baker, column 4, lines 36-46 and 53-56. However, the line 36-46 disclosure in Baker merely discloses use of a personal password unique to an individual, and the lines 53-56 disclosure merely discloses a user/user terminal of "the identified class." How or in what manner the class is "identified" has no antecedent basis and is not further explained in Baker. Clearly the required disclosure of the claim is not present in Baker or for that matter in Davis either.

More importantly, the Examiner admits, on page 4 of the Final Rejection that "Baker does not specifically disclose wherein the evidence of membership of the user group is authenticated evidence." The Examiner also admits "Baker doesn't discuss how the identification code is authenticated." These admissions are very much appreciated.

The Examiner attempts to recover from the admitted lack of teaching in Baker (and in Davis) by alleging that it is "extremely common and well known in the art." However, the Examiner provides no citation to support his contention which has been traversed by the appellant. Appellants previously noted the provisions of MPEP Section 2144.03 and traversed the Examiner's assertion that

the subject matter of the above-discussed "giving access" step is "extremely common and well known." The burden is on the Examiner to show where the giving access step is "in response to such member providing authenticated evidence of membership of that user group."

The failure to provide evidence showing where or how the "giving access" step is known or shown is a further indication of the lack of a prima facie case of obviousness.

5. The Examiner provides no "reason" or "motivation" for combining the Baker and Davis references

In view of the Examiner's admission that Baker does not disclose all features of Appellants' independent claims, the Examiner combines Baker with Davis. However, as noted above in *In re Rouffet* above, the Examiner has failed to meet his burden of proof by providing a "reason" or "motivation" for combining the Baker and Davis references.

Baker does not rely on or even mention evidence of "allocating" "human users" or any group membership and therefore has no reason to authenticate such user group membership. In fact, there is no motivation to even search for authentication of evidence of user group membership, because Baker ignores such user groups. Without some motivation for combination, the Baker/Davis combination and rejections based thereon fail.

6. The Examiner erroneously concludes that Davis discloses the claimed form of authentication, i.e., "membership of a user group [to be] . . . authentically evidenced."

Appellants independent claims each requires "membership of a user group [to be] . . . authentically evidenced." The Examiner alleges, in the official action at the bottom of page 4, that Davis does disclose "identification means comprises authenticated evidence" citing Davis page 553. the error in this contention is shown by reference to Davis on page 550, left column, last sentence of section B, where he specifically teaches that both parties "mutually authenticate." This is authentication of one individual's identity by another individual.

Mutual authentication may be what is disclosed in Davis, but this does not comprise any disclosure of the claimed "membership of a user group [to be] . . . authentically evidenced." Thus this feature is missing from Davis as well as Baker.

7. The Examiner also errs in concluding that Davis discloses "authenticated evidence" at page 553 under heading B

As noted above, the independent claims require "membership of a user group [to be] . . . authentically evidenced." The Examiner additionally contends that Davis discloses "authenticated evidence" by his use of "certificates" and cites page 553 under heading B. However, the cited portion of Davis merely teaches that the Davis certificate is authentication of **one individual's identity** and is not

authentication of evidence of membership of a **user group** as required by Appellants' independent claims.

Thus, the Examiner's conclusion as to the teachings of the Davis reference is respectfully traversed.

8. No prima facie case of obviousness of the independent claims 1, 19, 32, 35, 38, 40, 41 or 43-45 has been made out by the Examiner with respect to Baker and Davis

Claims 1-5, 11-13, 17, 19-23, 29, 31, 32, 38, 41, 44 and 45 are either independent or dependent (directly or indirectly) upon independent claims 1, 19, 32, 35, 38, 40, 41 or 43-45. As noted above (items A1-A4 with respect to Baker and items A6-A7 with respect to Davis), numerous structural elements, logic elements and method steps are recited in the independent claims and yet the Examiner fails to identify any teaching in the cited prior art references disclosing these claim features. The failure to disclose claimed elements in at least one of the cited references obviates any basis for a rejection under 35 USC §103.

Additionally, the Examiners failure to identify any "reason" or "motivation" to combine references (item A5) confirms that the burden to establish a *prima facie* case of obviousness has not been met.

Accordingly, the rejection of Claims 1-5, 11-13, 17, 19-23, 29, 31, 32, 38, 41, 44 and 45 in the Final rejection is not supported and any further rejection of these claims is respectfully traversed.

B. The Examiner fails to identify any evidence of record tending to support an obviousness rejection of claims 6, 24, 39 and 42 under §103 with the Baker/Davis combination in view of Hsiao

Claims 6, 24, 39 and 42 stand rejected under 35 USC §103 as unpatentable over the Baker/Davis combination taken with Hsiao. The above comments with respect to the Baker and Davis references, both separately and in combination, are herein incorporated by reference. Additionally, inasmuch as claims 6, 24, 39 and 42 are directly dependent upon independent claims 1, 19, 38 and 41, respectively, Appellants rely for patentability on the non-obviousness of the independent claims in view of the Baker and Davis references.

It is noted that at no point in the Final Rejection does the Examiner contend that the Hsiao reference supplies any feature, logic or method step which, as discussed above, is missing from the Baker and Davis references. Therefore, even if Baker, Davis and Hsiao were combined, they would not disclose the subject matter of claims 6, 24, 39 and 42.

Moreover, the Examiner has failed to provide any "reason" or "motivation" for combining these three references. The Examiner's admission that "Baker does not disclose wherein the labels are meta tags" (Final Rejection, page 11, line 3) is very much appreciated. Accordingly, any further rejection of claims 6, 24, 39 and 42 over the Baker/Davis/Hsiao combination is respectfully traversed.

C. The Examiner fails to identify any evidence of record tending to support an obviousness rejection of claims 7 & 25 under §103 with the Baker/Davis combination

Claims 7 and 25 stand rejected under 35 USC §103 as unpatentable over the Baker/Davis. The above comments with respect to the Baker and Davis references, both separately and in combination, are herein incorporated by reference. Additionally, inasmuch as claims 6, 24, 39 and 42 are directly dependent upon independent claims 1, 19, 38 and 41, respectively, Appellants rely for patentability on the non-obviousness of the independent claims in view of the Baker and Davis references.

Accordingly, any further rejection of claims 6, 24, 39 and 42 over the Baker/Davis/Hsiao combination is respectfully traversed.

D. The Examiner fails to identify any evidence of record tending to support an obviousness rejection of claims 8, 9, 26 and 27 under §103 with the Baker/Davis combination in view of Harn

Claims 8, 9, 26 and 27 stand rejected under 35 USC §103 as unpatentable over the Baker/Davis combination taken with Harn. The above comments with respect to the Baker and Davis references, both separately and in combination, are herein incorporated by reference. Additionally, inasmuch as claims 8, 9, 26 and 27 are dependent upon independent claims 1 and 19, Appellants rely for patentability on the non-obviousness of the independent claims in view of the Baker and Davis references.

It is noted that at no point in the Final Rejection does the Examiner contend that the Harn reference supplies any feature, logic or method step which, as discussed above, is missing from the Baker and Davis references. Therefore, even if Baker, Davis and Harn were combined, they would not disclose the subject matter of claims 8, 9, 26 and 27. Moreover, the Examiner has failed to provide any "reason" or "motivation" for combining these three references.

Accordingly, any further rejection of claims 8, 9, 26 and 27 over the Baker/Davis/Harn combination is respectfully traversed.

E. The Examiner fails to identify any evidence of record tending to support an obviousness rejection of claims 10, 28 and 34 under §103 with the Baker/Davis combination in view of McNabb

Claims 10, 28 and 34 stand rejected under 35 USC §103 as unpatentable over the Baker/Davis combination taken with McNabb. The above comments with respect to the Baker and Davis references, both separately and in combination, are herein incorporated by reference. Additionally, inasmuch as claims 10, 28 and 34are directly dependent upon independent claims 1, 19 and 32, respectively, Appellants rely for patentability on the non-obviousness of the independent claims in view of the Baker and Davis references.

It is noted that at no point in the Final Rejection does the Examiner contend that the McNabb reference supplies any feature, logic or method step which, as discussed above, is missing from the Baker and Davis references. Therefore, even

if Baker, Davis and McNabb were combined, they would not disclose the subject matter of claims 10, 28 and 34. Moreover, the Examiner has failed to provide any "reason" or "motivation" for combining these three references.

Accordingly, any further rejection of claims 10, 28 and 34 over the Baker/Davis/McNabb combination is respectfully traversed.

F. The Examiner fails to identify any evidence of record tending to support an obviousness rejection of claims 14-16, 30 and 33 under §103 with the Baker/Davis combination in view of Hayman

Claims 14-16, 30 and 33 stand rejected under 35 USC §103 as unpatentable over the Baker/Davis combination taken with Hayman. The above comments with respect to the Baker and Davis references, both separately and in combination, are herein incorporated by reference. Additionally, inasmuch as claims 14-16, 30 and 33 are dependent upon independent claims 1, 19 and 32, Appellants rely for patentability on the non-obviousness of the independent claims in view of the Baker and Davis references.

It is noted that at no point in the Final Rejection does the Examiner contend that the Hayman reference supplies any feature, logic or method step which, as discussed above, is missing from the Baker and Davis references. Therefore, even if Baker, Davis and Hayman were combined, they would not disclose the subject matter of claims 14-16, 30 and 33. Moreover, the Examiner has failed to provide any "reason" or "motivation" for combining these three references.

Accordingly, any further rejection of claims 14-16, 30 and 33 over the Baker/Davis/Hayman combination is respectfully traversed.

G. The Examiner fails to identify any evidence of record tending to support an obviousness rejection under §103 with the Baker/Davis/Hayman combination and Netscape

Claim 18 stands rejected under 35 USC §103 as unpatentable over the Baker/Davis/Hayman combination taken with Netscape. The above comments with respect to the Baker, Davis and Hayman references, both separately and in combination, are herein incorporated by reference. Additionally, inasmuch as claim 18 is ultimately dependent upon independent claim 1, Appellants rely for patentability on the non-obviousness of the independent claim in view of the Baker, Davis and/or Hayman references.

It is noted that at no point in the Final Rejection does the Examiner contend that the Netscape reference supplies any feature, logic or method step which, as discussed above, is missing from the Baker, Davis and Hayman references. Therefore, even if Baker, Davis, Hayman and Netscape were combined, they would not disclose the subject matter of claim 18. Moreover, the Examiner has failed to provide any "reason" or "motivation" for combining these three references.

Accordingly, any further rejection of claim 18 over the Baker/Davis/Hayman/Netscape combination is respectfully traversed.

H. The Examiner fails to identify any evidence of record tending to support an obviousness rejection of claim 35 under §103 with the Baker/Davis combination

Claim 35 stands rejected under 35 USC §103 as unpatentable over the Baker/Davis combination. The above comments with respect to the Baker and Davis references, both separately and in combination, are herein incorporated by reference.

Accordingly, any further rejection of claim 35 over the Baker/Davis combination is respectfully traversed.

VIII. CONCLUSION

The independent claims require the method step of "allocating" human users of a computer system and this feature is not shown in either the Baker of Davis references. Each of the independent claims requires providing access to user members "in response to such member providing authenticated evidence of membership of that user group." This feature is not shown in either the Baker or Davis references.

Additionally, the Baker reference fails to disclose any identification of "a data access category which is common to members of that user group" or an allocating step with respect to "human users." Davis fails to disclose "authenticated evidence of membership of that user group" and the Examiner erroneously concludes otherwise, as established above.

Because of these glaring failures of disclosure of steps, logic or elements recited in the independent claims, the Examiner has clearly failed to meet his burden of showing "some objective teaching in the prior art" with respect to claimed elements, logic and method steps. The Examiner also fails to meet his burden of showing "reasons" or a "motivation" for combining references in the manner claimed. Thus, as noted in detail above, the Examiner has failed to establish a *prima facie* basis of obviousness for any of claims 1-45 over the Baker/Davis combination by itself or in combination with the other cited references.

As a result of the above, there is simply no support for the rejections of Appellants' independent claims or claims dependent thereon under 35 USC §103. Thus, and in view of the above, the rejection of claims 1-45 is clearly in error and reversal thereof by this Honorable Board is respectfully requested.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____

Stanley C. Spooner
Reg. No. 27,393

SCS:kmm
Enclosure

IX. CLAIMS APPENDIX

1. (previously presented) A method for computer security to control access to data held on a computer system as requestable datasets, said method comprising the steps of:

allocating human users of a computer system between a plurality of user groups as members thereof wherein not all user groups have only a single member and membership of a user group having multiple members is authentically evidenced by provision of user group identity information common to such members, each user group corresponding to a respective dataset access category selected from a plurality of such categories such that all members of each user group having multiple members are associated with a dataset access category which is common to members of that user group;

providing for each dataset a dataset access category selected from said plurality of such categories and associated with a criterion for access to that dataset by computer system users; and

giving access to a dataset to a member of a user group with multiple members in response to such member providing authenticated evidence of membership of that user group and members of that user group being associated with a common dataset access category which enables access to that dataset.

2. (previously presented) A method according to Claim 1, wherein the user groups and data access categories have hierarchical levels in which a higher dataset access category incorporates a or, as the case may be, each lower dataset access category, and the method includes allowing access to datasets by members of user groups associated with dataset access category levels equal to and higher than those to which such datasets correspond.

3. (previously presented) A method according to Claim 1, wherein each user is associated with a computer-based identifying certificate means and the method includes the step determining a user's identity from the identifying certificate means.

4. (previously presented) A method according to Claim 3, wherein the computer-based identifying certificate means is an X.509 certificate.

5. (previously presented) A method according to Claim 1, wherein the datasets are web pages and the method includes the step of gaining access to the computer network via the Internet or the World-Wide-Web.

6. (original) A method according to Claim 1, wherein the datasets are web pages and the step of associating each dataset with a dataset access category comprises inserting meta tags in html web page code.

7. (previously presented) A method according to Claim 1, further including the step of performing a challenge-response exchange regarding user identification before the step of giving access to a dataset.

8. (previously presented) A method according to Claim 1 in which a user group member employs a user computer system to gain access to datasets to which access is controlled by an access control computer system having a public key for verifying signed data, wherein each user computer system incorporates a private key for signing data and user group identifying means, and the dataset access step includes:

using the private key to sign test data provided by the access control computer system and forwarding the signed data and user group identity information provided by the identifying means to the access control computer system; and

using the access control computer system to;

verify the user group identity information,

verify the user by using the public key to verify the signed data, and

determine user group and associated dataset access category from the user group identity information.

9. (original) A method according to Claim 8, wherein the test data is random data.

10. (original) A method according to Claim 1, further including the step of providing database access to a first kind of user having a user certificate for identification purposes and a second kind of user lacking such certificate.

11. (original) A method according to Claim 1, wherein data is maintained on at least one database computer system, dataset access is given by access control software operated on a separate access control computer system, and a user gains access to data by means of access request software running on a user computer system separate from the database and access control computer systems.

12. (original) A method according to Claim 11, wherein the access control software is configured with a firewall protecting a database computer system.

13. (previously presented) A method according to Claim 11, wherein data is maintained on a plurality of database computer systems and, in response to a data request, access control software determines whether or not corresponding data access is appropriate after relaying the request to a database computer system having such data.

14. (original) A method according to Claim 1, wherein data access categories and the user groups and datasets with which they are associated are assigned respective numerical values and the step of giving dataset access involves comparing user group and dataset numerical values to determine whether or not access is to be granted or denied.

15. (original) A method according to Claim 14, wherein the data access categories have different sections each with a section numerical value and the step of comparing numerical values comprises comparing section numerical values of corresponding sections of user group and dataset numerical values.

16. (original) A method according to Claim 14, wherein access to a dataset is provided only if all section comparisons are satisfied.

17. (original) A method according to Claim 1, wherein the step of giving access to a dataset includes unencrypted transfer of data from datasets to which access is granted.

18. (previously presented) A method according to Claim 16 wherein a user has a user computer system, and wherein the method includes the step of running checking/blocking software on the user computer system to screen incoming data for encryption to block unwanted data content.

19. (previously presented) A computer program product comprising a computer readable medium containing computer readable instructions for controlling operation of a computer system and providing control of access to data held on a computer system as requestable datasets each having an access category selected from a plurality of such categories and associated with a criterion for access to that dataset by computer system users, wherein the computer readable instructions provide a means for controlling the computer system to:

(a) receive data requests from human users of a computer system allocated between a plurality of user groups as members thereof wherein not all user groups have only a single member and membership of a user group having multiple members is authentically evidenced by provision of user group identity information common to such members, each user group being associated with a

respective one of said data access categories such that all members of a user group having multiple members are associated with a dataset access category which is common to members of that user group;

(b) control access to datasets each of which is associated with a dataset access category selected from said plurality of such categories and associated with a criterion for access to that dataset by computer system users; and

(c) give access to a dataset to a member of a user group with multiple members in response to such member providing authenticated evidence of membership of that user group and members of that user group being associated with a common dataset access category which enables access to that dataset.

20. (previously presented) A computer program product according to Claim 19, wherein the user groups and data access categories have hierarchical levels in which a higher dataset access category incorporates a or, as the case may be, each lower dataset access category, and the computer readable instructions allow access to datasets by members of user groups associated with dataset access category levels equal to and higher than those to which such datasets correspond.

21. (previously presented) A computer program product according to Claim 19, wherein the computer readable instructions provide a means for determining a user's identity from computer-based identifying certificate means.

22. (previously presented) A computer program product according to Claim 21, wherein the computer-based identifying certificate means is an X.509 certificate.

23. (original) A computer program product according to Claim 19, wherein the datasets are web pages and the computer readable instructions enable access to the web pages via the Internet or the World-Wide-Web.

24. (original) A computer program product according to Claim 19, wherein the datasets are web pages and the computer readable instructions provide a means for identifying dataset access categories in web pages from meta tags in html web page code.

25. (previously presented) A computer program product according to Claim 19, wherein the computer readable instructions provide a means for challenging incoming data requests regarding user identification before giving access to a dataset.

26. (previously presented) A computer program product according to Claim 19 for interacting with a user computer system incorporating a private key for signing data and user group identifying means, wherein the computer readable instructions provide a means for controlling the computer system to:

(a) send test data to the user computer system for signature with the private key and return with user group identity information provided by the identifying means,

(b) verify the user group identity information,

(c) verify the user by using the public key to verify the signed data, and

(d) determine user group and associated dataset access category from the user group identity information.

27. (original) A computer program product according to Claim 26, wherein the test data is random data.

28. (original) A computer program product according to Claim 19, wherein the computer readable instructions provide database access to a first kind of user having a user certificate for identification purposes and a second kind of user lacking such certificate.

29. (original) A computer program product according to Claim 19, wherein the computer readable instructions provide a firewall for a database computer system.

30. (original) A computer program product according to Claim 19, wherein data access categories and the user groups and datasets with which they are associated are assigned respective numerical values and the computer readable instructions provide a means for granting or denying dataset access on the basis of comparison of user group and dataset numerical values.

31. (original) A computer program product according to Claim 19, wherein the computer readable instructions provide a means for transferring dataset material to appropriate recipients unencrypted.

32. (previously presented) A network access controller for controlling access to data held on a computer system as requestable datasets, wherein the controller:

(a) receives data requests from human users of a computer system allocated between a plurality of user groups as members thereof wherein not all user groups have only a single member and membership of a user group having multiple members is authentically evidenced by provision of user group identity

information common to such members, each user group corresponding to a respective dataset access category selected from a plurality of such categories such that all members of each user group having multiple members are associated with a dataset access category which is common to members of that user group;

(b) controls access to datasets each of which is associated with a dataset access category selected from said plurality of such categories and associated with a criterion for access to that dataset by computer system users; and

(c) gives access to a dataset to a member of a user group with multiple members in response to such member providing authenticated evidence of membership of that user group and members of that user group being associated with a common dataset access category which enables access to that dataset.

33. (original) A controller according to Claim 32, wherein the controller compares numerical values associated with data access categories of datasets and user groups in order to determine whether or not to grant access to data.

34. (original) A controller according to Claim 32, wherein said controller provides database access to a first kind of user having a user certificate for identification purposes and a second kind of user lacking such certificate.

35. (previously presented) A computer network for database access by human users having identifying certificates and allocated between a plurality of user groups as members thereof wherein not all user groups have only a single member and membership of a user group having multiple members is authentically evidenced by provision of user group identifying certificate information common to such members, wherein said network treats each user group as corresponding to a respective dataset access category selected from a plurality of such categories such that all members of each user group having multiple members are associated with a dataset access category which is common to members of that user group, and includes:

(a) an access controller controlling access to a database comprising a plurality of datasets each having an associated dataset access category selected from said plurality of such categories and associated with a criterion for access to that dataset by users;

(b) means for verifying human users;

(c) a database of datasets each of which is associated with a dataset access category selected from said plurality of such categories; and

(d) computer software arranged to give access to a dataset to a member of a user group with multiple members in response to such member providing identifying certificate information as evidence of membership of that user group

and members of that user group being associated with a common dataset access category which enables access to that dataset.

36. (original) A network according to Claim 35, wherein the database comprises web pages in which dataset access categories are implemented by insertion of meta tags in web page html code.

37. (original) A network according to Claim 35, wherein said network is an Internet or World-Wide Web network.

38. (previously presented) A method for controlling user access to data held on a computer system as requestable datasets, the method including:

labelling the datasets with dataset access labels defining a hierarchy of data access levels each associated with a criterion for access to a dataset by computer system users,

allocating human users of a computer system between a plurality of user groups as members thereof wherein not all user groups have only a single member and membership of a user group having multiple members is authentically evidenced by provision of user group identity information common to such members,

labelling user groups with data access levels selected from said plurality thereof such that all members of each user group having multiple members are associated with a dataset access level which is common to members of that user group; and

giving access to a requested dataset to a requesting member of a user group with multiple members in response to such member providing authenticated evidence of membership of that user group and members of that user group being labelled with a common data access level which in the hierarchy is equal to or above the dataset access level of the requested dataset.

39. (previously presented) A method according to claim 38 wherein the datasets are web pages with dataset access labels which are meta tags, and a proxy server is used to:

receive requests for web pages from members of user groups,

check user group data access levels against a prearranged access control list, and

deny members of a user group access to requested web pages if they lack a data access level appearing on the access control list.

40. (previously presented) A method for controlling user access to data held on a computer system as requestable web pages, the method including:

(a) labelling the web pages with meta tags defining a hierarchy of data access levels for an access control list providing a plurality of data access levels each associated with a criterion for access to a dataset by computer system users,

(b) allocating human users of a computer system between a plurality of user groups as members thereof wherein not all user groups have only a single member and membership of a user group having multiple members is authentically evidenced by provision of user group identity information common to such members, each member having a key for signing data and a certificate indicating groupings to which that member belongs,

(c) labelling user groups with respective data access levels associated with member groupings and selected from said plurality thereof such that all members of each user group having multiple members are associated with a dataset access level which is common to members of that user group,

(d) using a proxy server to:

receive a request for a web page from a client computer system having web browser software and client proxy software and controlled by a requesting member of a user group,

send data for signature to the client computer system and obtain the requesting member's certificate,

receive data from the client computer system,

verify that the received data is:

(1) signed with the requesting member's key,

(2) a signed equivalent of the data sent to the requesting member for signature, and

(3) signed with a key from a certificate which is not time expired or invalid,

if the received data is verified as aforesaid, check the data access level of the requesting member's user group against the access control list, and

give access to a requested web page to the requesting member if said requesting member is a member of a user group with multiple members in response to such member providing authenticated evidence of membership of that user group and members of that user group being labelled with a common data access level which in the hierarchy is equal to or above the dataset access level of the requested web page.

41. (previously presented) A network access control system for controlling access to data held on a computer system as requestable datasets, the control system being arranged to:

(a) label the datasets with dataset access labels defining a hierarchy of data access levels,

(b) communicate with human computer system users allocated between a plurality of human user groups,

(c) label said user groups with data access levels selected from a plurality of such levels; and

(d) give access to a requested dataset to a requesting human member of a user group labelled with a data access level which in the hierarchy is equal to or above the data access level of the requested dataset.

42. (previously presented) A network access control system according to claim 41 wherein the datasets are web pages with dataset access labels which are meta tags and the control system has a proxy server for:

(e) receiving requests for web pages from members of user groups,

(f) checking user group data access levels against a prearranged access control list, and

(g) denying members of a user group access to requested web pages if they lack a data access level appearing on the access control list.

43. (previously presented) A network access control system for controlling user access to data held on a computer system as requestable web pages, the control system being arranged to:

(a) label the web pages with meta tags defining a hierarchy of data access levels for an access control list providing a plurality of data access levels each associated with a criterion for access to a dataset by computer system users,

(b) allocate human users of a computer system between a plurality of user groups as members thereof wherein not all user groups have only a single member and membership of a user group having multiple members is authentically evidenced by provision of user group identity information common to such members, each member having a key for signing data and a certificate indicating groupings to which that member belongs,

(c) label user groups with respective data access levels associated with member groupings and selected from said plurality of member groupings such that all members of each user group having multiple members are associated with a dataset access level which is common to members of that user group,

and the control system has a proxy server for:

(i) receiving a request for a web page from a client computer system having web browser software and client proxy software and controlled by a requesting member of a user group,

(ii) sending data for signature to the client computer system and obtain the requesting member's certificate,

(iii) receiving data from the client computer system,

(iv) verifying that the received data is:

signed with the requesting member's key,

a signed equivalent of the data sent to the requesting member for signature, and

signed with a key from a certificate which is not time expired or invalid,

(v) if the received data is verified as aforesaid, checking the data access level of the requesting member's user group against the access control list, and

(vi) giving access to a requested web page to the requesting member if it is a member of a user group with multiple members in response to such member providing authenticated evidence of membership of that user group and members of that user group being labelled with a common data access level which in the hierarchy is equal to or above the dataset access level of the requested web page.

44. (previously presented) A method for computer security to control access to data held on a computer system as requestable datasets, the method including:

(a) allocating human users of a computer system between a plurality of user groups as members thereof wherein not all user groups have only a single member and membership of a user group having multiple members is authentically evidenced by provision of user group identity information common to such members;

(b) providing for each dataset an access category selected from a plurality of such categories and associated with a criterion for access to that dataset by

computer system users, the dataset access categories being arranged in a hierarchy such that a relatively higher dataset access category incorporates one or more relatively lower dataset access categories;

(c) associating each user group with a respective dataset access category such that all members of each user group having multiple members are associated with a dataset access category which is common to members of that user group and membership of a user group having multiple members is authentically evidenced by provision of like user group information by each of such multiple members; and

(d) providing access to a dataset to a member of a user group with multiple members in response to such member providing authenticated evidence of membership of that user group and members of that user group being associated with a common dataset access category which is in the hierarchy equal to or relatively higher than that required for access to that dataset.

45. (previously presented) A method for computer security to control access to data held on a computer system as requestable datasets characterised in that the method includes:

(a) allocating human users of a computer system between a plurality of user groups as members thereof wherein not all user groups have only a single member and membership of a user group having multiple members is authentically

evidenced by provision of user group identity information common to such members;

(b) providing for each dataset an access category selected from a plurality of such categories and associated with a criterion for access to that dataset by computer system users, the dataset access categories being arranged in a hierarchy such that a relatively higher dataset access category incorporates one or more relatively lower dataset access categories;

(c) associating each user group with a respective dataset access category such that all members of each user group having multiple members are associated with a dataset access category which is common to members of that user group;

(d) providing a respective computer-based identifying certificate means for each user containing said user group identity information; and

(e) providing access to a dataset to a member of a user group with multiple members in response to such member providing identifying certificate means and members of that user group being associated with a common dataset access category which is in the hierarchy equal to or relatively higher than that required for access to that dataset.

X. EVIDENCE APPENDIX

None.

XI. RELATED PROCEEDINGS APPENDIX

None.